UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,129	09/10/2003	David G. Therrien	25452-013	3559

30623 7590 05/29/2008

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ATTN: PATENT INTAKE CUSTOMER NO. 30623
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
ADAMS, CHARLES D	
ART UNIT	**PAPER NUMBER**
2164	

MAIL DATE	DELIVERY MODE
05/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/659,129	THERRIEN ET AL.	
	Examiner	Art Unit	
	CHARLES D. ADAMS	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-17 and 19-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-17 and 19-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7 March 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 6 February 2008, claim 10 is amended. Claims 1, 3-17, and 19-26 are pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 6, 17, and 21-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395) in view of Zayas et al. (US Patent 6,560,615).

As to claim 1, Whiting et al. teaches a data protection system, comprising:

A fileserver configured to contain shares of data and to be connected with a repository, wherein the repository is configured to store a replica of a file (see 7:8-19 and 7:59-8:20);

The fileserver includes:

A filter driver operative to intercept input or output activity initiated by client file requests (see 7:8-19 and 7:59-8:20)

Whiting et al. does not teach and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred.

Zayas et al. teaches and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred (see 5:31-40 and 7:16-46);

Whiting et al. as modified teaches a file system in communication with the filter driver and operative to store client files (see Zayas et al. 7:16-46 and Whiting et al. 7:8-19);

The filter driver is configured to capture the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the fileserver (see Whiting et al. 5:2-8).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

As to claim 6, Whiting et al. as modified teaches: wherein the fileserver, based on the protection policy, is adapted to define repositories used for storage of files (see Whiting et al. 7:59-8:20), frequency of data backup (see Whiting et al. 5:2-8 and 33:49-

51), how many replicas are maintained within each repository (see Whiting et al. 8:16-20), and how modifications to share data are maintained (see Whiting et al. 7:59-8:20).

As to claim 17, Whiting et al. teaches a data protection system comprising:

A fileserver configured to contain shares of data and to be connected with a repository, wherein the repository is configured to store a replica of a file (see 7:8-19 and 7:59-8:20);

Said fileserver includes:

Filter driver means for intercepting input or output activity initiated by client file requests (see 7:8-19 and 7:59-8:20)

Whiting et al. does not teach and for capturing a snapshot of a set of the shares of data at a particular point in time and for maintaining a list of modified and/or created files since a last snapshot occurred

Zayas et al. teaches and for capturing a snapshot of a set of the shares of data at a particular point in time and for maintaining a list of modified and/or created files since a last snapshot occurred (see 5:31-40 and 7:16-46)

Whiting et al. as modified teaches:

File system means in communication with the filter driver, the file system means for storing client files (see Zayas et al. 7:16-46 and Whiting et al. 7:8-19);

Wherein said filter driver means is configured to capture the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the file server (see Whiting et al. 5:2-8).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

As to claim 21, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine whether to purge a file from a repository after the file has been deleted from a set of files (see Zayas et al. 7:11-15 and 8:5-14).

As to claim 22, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine whether to keep a version history of a file in the set of files (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 23, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified backup frequency for a repository (see Whiting et al. 5:2-8 and 33:49-51).

As to claim 24, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified type of compression for a file in the set of files (see Whiting et al. 8:21-40).

As to claim 25, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified caching level of a repository (see Whiting et al. 6:52-7:2).

4. Claims 3-5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395) in view of Zayas et al. (US Patent 6,560,615), and further in view of Belknap et al. (US Pre-Grant Publication 2003/0070001).

As to claim 3, Whiting et al. as modified teaches the system of claim 1.

Whiting et al. as modified does not teach a location cache configured to determine based on the protection policy which repository will be used to protect each share of data;

Belknap et al. teaches a location cache configured to determine based on the protection policy which repository will be used to protect each share of data (see paragraphs [0063]-[0064]).

Whiting et al. as modified teaches a location manager coupled to the location cache and operative to update the location cache when the fileserver protects a new share of data in a specific repository node (see Belknap et al. paragraph [0069]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Belknap et al., since Belknap et al. teaches "to provide a common interface to media servers which conceals the media server specific device commands from applications which interact with the media servers included within the system" (see paragraph [0006]).

As to claim 4, Whiting et al. as modified teaches:

A local repository in communication with the fileserver and adapted for receiving files from the fileserver (see Whiting et al. 7:59-8:20. Whiting et al. transfers items from a local database to a remote one):

A local repository node API adapted for communicating with the fileserver API (see Whiting et al. 7:59-8:20);

The local repository is further adapted to receive replicated files from the fileserver (see Whiting et al. 7:59-8:20); and

The local repository includes a protection policy component operative to determine whether new versions of existing files should be compressed and whether older versions of exiting files should be maintained (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 5, Whiting et al. as modified teaches:

A remote repository in communication with the local repository and adapted for receiving files from the local repository (see Belknap et al. paragraph [0066] and Whiting et al. 6:52-7:2):

The remote repository is further adapted to receive replicated files from the local repository (see Belknap et al. paragraph [0066] and Whiting et al. 6:52-7:2);

The remote repository includes a protection policy component operative to determine whether new versions of existing files should be compressed and whether older versions of existing files should be maintained (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 20, Whiting et al. teaches the system of claim 1.

Whiting et al. does not teach wherein, based in the protection policy, the fileserver is configured to determine the location of repositories

Belknap et al. teaches wherein, based in the protection policy, the fileserver is configured to determine the location of repositories (see paragraphs [0063]-[0064])

Whiting et al. as modified teaches and a number of replicas of the files to be stored in each repository (see Whiting et al. 8:16-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Belknap et al., since Belknap et al. teaches “to provide a common interface to media servers which conceals the media server specific device commands from applications

which interact with the media servers included within the system" (see paragraph [0006]).

5. Claims 7-10, 13-16, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al. (US Patent 6,847,982) in view of Zayas et al. (US Patent 6,560,615).

As to claim 7, Parker et al. teaches a method for protecting data comprising:

Storing a version of a file within a set of files on a primary disk storage system (see 7:24-35);

Parker et al. does not teach capturing a snapshot of the set of files at a particular point in time

Zayas et al. teaches capturing a snapshot of the set of files at a particular point in time (see 7:16-46);

Parker et al. as modified teaches based on a backup frequency defined in a protection policy (see Parker et al. 7:32-34 and 9:6-11);

Maintaining a list of modified and/or created files since last captured snapshot (see Zayas et al. 5:31-40 and 7:16-46);

Examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files (see Parker et al. 7:34-35 and 9:23); and

Replicating the version of the file to a repository specified by the protection policy, wherein the repository includes at least one of a local repository and a remote repository (see Parker et al. 7:44-59 and 9:23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Parker et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

As to claim 8, Parker et al. teachers wherein the file is configured to have at least one version (see Parker et al. 8:17-25 and Zayas et al. 6:65-7:15).

As to claim 9, Parker et al. teaches applying reverse delta compression to the versions of the file when a successive version of the file is stored in the repository (see Parker et al. 9:54-10:4).

As to claim 10, Parker et al. teaches wherein the step of applying reverse delta compression comprises:

Creating another version of the file, wherein the another version of the file is in a version of the file successive to the version of the file (see Parker et al. 9:54-10:4);

Replicating the another version of the file into the local repository and the remote repository (see Parker et al. 6:42-59 and 9:54-10:4);

Replacing the replicated version of the file in the local repository with a reverse delta compressed version representing a difference between the version of the file and the another version of the file and replicating; (see Parker et al. 9:54-10:4)

Transmitting the reverse delta compressed version to the remote repository (see Parker et al. 6:42-59. A reverse delta can be sent with the data with the shipping container as well as a forward delta); and

In the remote repository, replacing the version of the file with the reverse delta compressed version to store the another version and the reverse delta compressed version (see Parker et al. 6:42-59 and Zayas et al. 7:25-32. A reverse delta can be sent with the data with the shipping container as well as a forward delta).

As to claim 13, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to keep a version history of a file in the set of files (see Zayas et al. 7:25-40 and Parker et al. 9:54-10:4).

As to claim 14, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified backup frequency for a repository (see Parker et al. 8:17-25 and 9:6-11).

As to claim 15, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified type of compression for a file in the set of files (see Parker et al. 6:42-59. A reverse delta can be chosen along with a forward delta to send to the library).

As to claim 16, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified caching level of a repository (see Parker et al. 9:12-14. A storing (caching) frequency level is determined and chosen).

As to claim 26, Parker et al. as modified teaches wherein the fileserver further includes:

backup means for backing up the modified files into repositories identified in the protection policy based on the backup frequency (see Parker et al. 9:6-11);

Storage means for storing a latest version of a file in a repository where a prior version of the file is stored (see Parker et al. 9:54-10:4);

Means for determining a difference between the latest version of the file and the prior version of the file (see Parker et al. 9:54-10:4);

Means for applying reverse delta compression of the difference (see Parker et al. 9:54-10:4); and

Means for replacing the prior version of the file with the reverse delta compressed difference between the latest version and the prior version of the file (see Parker et al. 9:54-10:4).

6. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al. (US Patent 6,847,982) in view of Zayas et al. (US Patent 6,560,615), and further in view of Santry et al. ("Deciding when to forget in the Elephant file system").

As to claim 11, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining the location of repositories (see Parker et al. 10:36-55)

Parker et al. does not teach and a number of replicas of the files to be stored in each repository.

Santry et al. teaches a number of replicas of the files to be stored in each repository (see page 113, section 3.3. Only one version is kept).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to have modified Parker et al. by the teaching of Santry et al., since

Santry et al. teaches that "old versions of files are automatically retained and storage is managed by the file system. Users specify retention policies for individual files, groups of files, or directories. The goal of Elephant is to allow users to retain important old versions of all of their files. User actions such as delete and file write are thus easily revocable by rolling back a file system, a directory, or an individual file to an earlier point in time" (see page 111, last paragraph of section 1).

As to claim 12, Parker et al. teaches the method of claim 7.

Parker et al. does not teach wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to purge a file from a repository after the file has been deleted from a set of files.

Santry et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to purge a file from a repository after the file has been deleted from a set of files (see page 113, section 3.5 and 115, section 4.2.3 (it is determined whether a file should be deleted)).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to have modified Parker et al. by the teaching of Santry et al., since Santry et al. teaches that "old versions of files are automatically retained and storage is

managed by the file system. Users specify retention policies for individual files, groups of files, or directories. The goal of Elephant is to allow users to retain important old versions of all of their files. User actions such as delete and file write are thus easily revocable by rolling back a file system, a directory, or an individual file to an earlier point in time" (see page 111, last paragraph of section 1).

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395) in view of Zayas et al. (US Patent 6,560,615), and further in view of Burns et al. ("Efficient Distributed Backup with Delta Compression").

As to claim 19, Whiting et al teaches:

Backup said modified files into repositories identified in said protection policy based on said backup frequency (see Whiting et al. 5:2-8 and 33:49-51);

Store a latest version of a file in a repository where a prior version of said file is stored (see Whiting et al. 8:21-31);

Determine a difference between said latest version of said file and said prior version of said file (see Whiting et al. 8:21-31);

Whiting et al. does not teach to apply reverse delta compression to said difference;

Burns et al. teaches to apply reverse delta compression to said difference (see Burns et al. section 4.2);

Whiting et al. as modified teaches replace said prior version of said file with said reverse delta compressed difference between said latest version and said prior version of said file (see Burns et al. section 4.2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Burns et al., since Burns et al. teaches that "by using delta compression algorithms, which minimally encode a version of a file using only the bytes that have changed, a backup system can compress the data sent to a server" (see Abstract).

Response to Arguments

8. Applicant's arguments filed 7 March 2008 have been fully considered but they are not persuasive.

In regards to claim 1, Applicant argues that the teachings of Whiting et al. are "different than the filter driver that is configured to capture the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the fileserver". In response to this argument, it is noted that, as pointed out by Applicant, Whiting et al. teaches that backups can occur automatically or independently for each node and can be scheduled by the user or administrator (see 5:6-8). It is also noted that Whiting et al. teaches that the user may schedule periodic backups (see 35:64-36:4).

Applicant also argues that "Whiting fails to disclose, teach, or suggest a fileserver configured to contain shares of data and to be connected with a repository, wherein the repository is configured to store a replica of a file, as recited in amended claim 1. In contrast, Whiting only creates and modifies files on the backup storage. This is different from present invention's a fileserver connected to a repository that stores a replica of a file. Whiting only deals with four categories of files: new, unchanged, updated, or modified, but fails to teach file replicas being stored on repositories". It is noted that a 'repository' is a file storage. It is noted that the backup storage of Whiting et al. is a repository. It is also noted that the files that Whiting et al. "only creates and modifies" on the backup storage are backups of files. Therefore, they are "file replicas" (see 7:59-8:20).

Applicant also argues "Whiting's client systems are the source of backup data and a fileserver acts as a destination of backup data. Whiting maintains a replica of data from client systems that are spread out over the network into their destination fileserver. This is in contrast to the present invention, where the fileserver is the source of backup and a repository is the destination of backup. The present invention maintains a replica of all fileserver data in a repository. Thus, the fileserver and the repository are parts of the system in the present invention." In response to this argument, it is noted that the client systems and file servers of Whiting et al. that are the source of backup data are functionally equivalent to the fileserver that is a part of the system in the present application. It is also noted that the backup storage of Whiting et al. is functionally

equivalent to the repository of the present invention. The elements of Whiting et al. are connected in a system, as are the elements of the present invention.

Applicant argues that "Further, Whiting does not include a filter driver that is logging changes to a file as they happen. Whiting fails to disclose how files are subdivided into the four categories mentioned above. This is in contrast to the present invention that continually tracks all changes to the file system located on the fileserver as the files are modified so that when a snapshot is taken, there is a complete list of the files that have to be backed up available". In response to this argument, it is noted that the claim language states "a filter driver operative to intercept input or output activity initiated by client file requests". It is noted that Whiting et al. teaches to monitor changes to files and determine which files have been updated or created or deleted. This is 'intercepting input activity' (see 7:8-19 and 7:59-8:20).

Applicant argues that "the present invention captures a snapshot of an entire file system at a specific point in time. Such snapshots are taken at specific periods of time and lists of files are maintained since last snapshot and not since last archive, as taught by Zayas". In response to this argument, it is noted that both taking a snapshot of data that has been modified since a prior snapshot and archiving files that have been modified since a prior backup are functionally equivalent. "Further, Zayas appears to enumerate and order only specific identified files, rather than modified and/or created files of claim 1". It is noted that the 'identified files' that applicant returns to are files that

are included in a modified file list, referred to in Zayas et al. as an MFL. This is a list that contains modified files (see Zayas et al. 5:31-40 and 7:16-46). This clearly meets the teaching of "maintaining a list of modified and/or created files since the last snapshot occurred".

Applicant also argues that "these identified files only relate to those files that were modified prior to the selected epoch. Once Zayas archives the files, entries corresponding to the files are removed from the modified file list. In contrast, the present invention captures a snapshot of a set of shares of data at a particular point in time, rather than capturing specific identified files". In response to this argument, Examiner notes that "a set of shares of data" is functionally equivalent to "specific identified files". It is also noted that Zayas et al. adds entries to the MFL once a file is modified or created, which is different than applicant's arguments that "these identified files only relate to those files that were modified prior to the selected epoch". Applicant also adds "further, the present invention maintains a list of files since last snapshot and does not remove any files from the lists". In response to this argument, Examiner notes that this limitation is not present in the claims.

Applicant argues that "Zayas's MFL is a persistent metadata storage structure that is maintained for the life of a volume contained on the storage structure. The present invention's list of new and modified files is maintained for just a single backup period and then the modified file list and the snapshot are deleted". In response to this

argument, Examiner notes that no limitation stating such qualities of the present invention is found in the claims.

Applicant also argues that “additionally, Zayas discusses end user primary storage data being deleted and the subsequent ramifications of that deletion on Zayas’ MFL, which is irrelevant to backup retention management. In contrast, in the present invention, an end-user deletion activities (similar to those discussed in Zayas) have no effect on the retention of data in the repository”. In response to this argument, Examiner notes that no limitation to this effect is present in the claims.

Applicant then argues that "the improper combination of Whiting and Zayas fails to disclose, teach or suggest, *inter alia*, a fileserver configured to contain shares of data and the be connected with a repository, wherein the repository is configured to store a replica of a file", and proceeds to list out the limitations of claim 1. Examiner notes that Whiting et al., in view of Zayas et al., do teach these limitations as described previously.

Applicant argues that “one of the major differences between Whiting and the present invention is that the present invention leverages backup data it already has to act as a second tier of data storage". In response to this argument, it is noted that no such limitation regarding a second tier of data storage is present in the claims. Applicant also argues that “Whiting treats these two data management applications as separate entities with backup data going to a disk repository and archive/HSM data going to tape

or optical disk". In response to this argument, it is noted that no such limitations regarding the nature of the two data management applications as separate entities appear in the claims.

Applicant argues that "Belknap fails to disclose a location cache. Instead, Belknap's invention provides an abstraction layer to allow any kind of object storage device to be used for storing media files (audio/video) files. This is different than the present invention that deals with homogenous server/magnetic disk drive systems that can be load balanced over time. The location cache provides a level of indirection that allows data stored within a specific repository node to be moved to a different node under circumstances of cross-repository server-capacity or performance imbalance". In response to this argument, it is noted that the claim limitation only states "a location cache configured to determine based on the protection policy which repository will be used to protect each share of data and a location manager coupled to the location cache and operative to update the location cache when the fileserver protects a new share of data in a specific repository node" Belknap et al. teaches this in paragraphs [0063]-[0064].The remainder of Applicant's arguments are directed towards subject matter not present in the claim language.

Applicant argues that neither Belknap et al. nor Burns et al. teach the subject matter of claim 1. In response to this argument, it is noted that neither Belknap et al. nor Burns et al. is relied upon to teach the subject matter of claim 1.

Applicant argues in regards to claim 7 that "Instead, Parker's Akashic File Clerk that contains signatures of files, runs an inventory on the changed files, and then stores the files in the Akashic Vault, but does not capture a snapshot of the set of files nor does it examine a protection policy and determine where and how to protect files". It is noted that Parker et al. does teach capturing a snapshot of the set of files and it does examine a protection policy to determine where and how to protect the files (see 7:24-35). Applicant argues that Parker et al. is different than "replicating the version of the file to a repository, specified by the protection policy, wherein the repository includes at least one of a local repository and a remote repository". It is noted that Parker et al. replicates a file to the Akashic vault, as specified by a protection policy. The Akashic vault then can sent a file to an offsite library system (a remote repository) (see 7:24-35 and 7:44-59).

Applicant argues that "Parker doesn't deal with storing historical versions of data over time". It is noted that Parker et al. creates backups and archives those snapshots. Backups are historical versions of data over time. Applicant further argues that "Parker's replication source and destination are not peers in terms of performance/cost/reliability ... this is different than the present invention, one of the advantages of which is that it supports a local and remote repository with identical storage capacity/performance/cost and reliability - servers with storage". It is noted that no such limitation appears in the claims.

Applicant argues that "Additionally, Parker must maintain a database of the running history of all files and how this database helps to determine which files have been changed, deleted, or added. In the present invention, by tracking all file system create, write, and delete operations in real time, there is no need to maintain a database of what's been backed, in contrast to Parker". In response to this argument, Examiner notes that there is no limitation prohibiting the use of such a database in the claims.

Applicant argues that "specifically, Zayas fails to disclose, teach, or suggest, *inter alia*, capturing a snapshot of the set of files at a particular point in time based on a backup frequency defined in a protection policy and maintaining a list of modified and/or created files since last captured snapshot". In response to this argument, it is noted that Zayas et al. does teach the stated limitations, as noted in the rejection above.

Applicant argues that Santry et al. does not teach the subject matter of claim 7.

Examiner notes that Santry et al. is not relied upon to teach the subject matter of claim 7.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHARLES D. ADAMS whose telephone number is (571)272-3938. The examiner can normally be reached on 8:30 AM - 5:00 PM, M - F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. D. A./
Examiner, Art Unit 2164

/Charles Rones/
Supervisory Patent Examiner, Art Unit 2164